Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (PREVIOUSLY PRESENTED) In a computer system, a method for securing access to data, comprising:

generating a first message at a first computer system, said first message comprising information corresponding to data, and transmitting said first message to a second computer system;

receiving said first message at said second computer system, and generating a key pair comprising an encode key and a decode key for encoding and decoding of said data;

generating a second message comprising said encode key, and transmitting said second message to said first computer system; and

receiving said second message at said first computer system, wherein said encode key in said second message is used to encode said data.

2. (PREVIOUSLY PRESENTED) The method of claim 1 further comprising:

storing said key pair and said information in said first message in a database record.

3. (PREVIOUSLY PRESENTED) The method of claim 1 further comprising:

encoding said data using said encode key, and storing said encoded data.

4. (PREVIOUSLY PRESENTED) The method of claim 1 wherein said first computer system comprises at least one client computer system and said second computer system comprises at least one server computer system.

5. (PREVIOUSLY PRESENTED) The method of claim 1 wherein said generating said first message further comprises:

generating a one way hash function associated with said data; and

placing said one way hash function, information identifying said data, and user information associated with a user of said data at said first computer system in said first message.

6. (PREVIOUSLY PRESENTED) The method of claim 5 further comprising:

obtaining said first message at said second computer;

generating a time stamp and a digital signature representing, said digital time stamp, and said one way hash function in said first message; and

storing said user information, said information identifying said data, said one way hash function, said one way time stamp and said digital signature.

7. (ORIGINAL) The method of claim 6 wherein said second message further comprises:

said time stamp, said information identifying said data, and said digital signature in said second message.

8. (CURRENTLY AMENDED) The method of claim 3 further comprising:

providing access to said encoded data by performing steps comprising:

generating a third message at said first computer system, said third message comprising information corresponding to said encoded data, and transmitting said third message to said second computer system;

receiving said third message at said second computer system, and using said information in said third message to retrieve a record corresponding to said encoded data, said record comprising ~~a~~said decode key for decoding said encoded data;

generating a fourth message comprising said decode key, and transmitting said fourth message to said first computer system;

receiving said fourth message at said first computer system, wherein said decode key in said fourth message ~~are~~is utilized to decode said encoded data.

9. (PREVIOUSLY PRESENTED) The method of claim 8 further comprising:

accessing said encoded data and decoding said encoded data using said decode key.

10. (CURRENTLY AMENDED) The method of claim 8 wherein said third message further comprises:

said information identifying said encoded data, said user information, and a~~said~~ digital signature.

11. (PREVIOUSLY PRESENTED) The method of claim 10 further comprising:

receiving said third message at said second computer system;

accessing said corresponding record; and

verifying said digital signature therein with said received digital signature.

12. (PREVIOUSLY PRESENTED) The method of claim 11 further comprising:

upon proper verification, generating a fourth message comprising information identifying said encoded data file and said decode key, and transmitting said fourth message to said first computer.

13. (PREVIOUSLY PRESENTED) The method of claim 12 further comprising:

receiving said fourth message at the first computer;

accessing said encoded data; and

using said decode key in said fourth message to decode said encoded data.

14. (PREVIOUSLY PRESENTED) The method of claim 11 further comprising:

upon successful verification, generating a data retrieval time stamp and storing said data retrieval time stamp.

15. (PREVIOUSLY PRESENTED) The method of claim 14 further comprising:

upon unsuccessful verification, generating an attempted data retrieval time stamp and storing said attempted data retrieval time stamp.

16. (CURRENTLY AMENDED) In a network system, a method of providing access to encoded data, comprising:

generating a first message at a first computer system, said first message comprising information corresponding to said encoded data, and transmitting said first message to a second computer system;

receiving said first message at said second computer system, and using said information in said first message to retrieve a record corresponding to said encoded data, said record comprising a decode key for decoding said encoded data, said decode key differing from an encode key used to generate said encoded data;

generating a second message comprising said decode key, and transmitting said second message to said first computer system;

receiving said second message at said first computer system, wherein said decode key in said second message ~~are~~is utilized to decode said encoded data.

17. (ORIGINAL) The method of claim 16 further comprising;

accessing said encoded data and decoding said encoded data using said decode key.

18. (ORIGINAL) The method of claim 16 wherein said first computer system comprises at least one client computer system and said second computer system comprises at least one server computer system.

19. (ORIGINAL) A system for securing access to data, comprising:

a first computer system interconnected to a second computer system via a communication link, wherein said first and said second computer systems are configured to perform steps comprising:

generating a first message at said first computer system, said first message comprising information corresponding to said data, and transmitting said first message to said second computer system;

B1

receiving said first message at said second computer system, and generating a key pair comprising an encode key and a decode key for encoding and decoding of said data;

storing said decode key in a record;

generating a second message comprising said encode key, and transmitting said second message to said first computer system; and

receiving said second message at said first computer system, wherein said encode key in said second message can be used to encode said data to secure access to said data.

20. (ORIGINAL) The system of claim 19, wherein said first computer is further configured to use said encode key to encode said data, and store said encoded data.

21. (CURRENTLY AMENDED) The system of claim 19, wherein said first and said second computer systems are further configured for providing access to encoded data by performing steps comprising:

generating a third message at said first computer system, said third message including information corresponding to said encoded data, and transmitting said third message to said second computer system;

receiving said third message at said second computer system, and using said information in said third message to retrieve a record corresponding to said encoded data, said record including asaid decode key for decoding said encoded data;

generating a fourth message comprising said decode key, and transmitting said fourth message to said first computer system;

receiving said fourth message at said first computer system, wherein said decode key in said fourth message can be utilized to decode said encoded data.

22. (CURRENTLY AMENDED) The system of claim 21, wherein said first computer is further configured to access said ~~encode~~encoded data and use said decode key to decode said encoded data.

23. (PREVIOUSLY PRESENTED) In a computer system, a method for providing secure real time storage and retrieval of file data comprising:

obtaining a secure save command from a user operating a screen element of a first computer system;

executing said secure save command to securely save file data at said first computer system, said executing comprising:

generating a first message at said first computer system, said first message comprising information corresponding to said file data, and transmitting said first message to a second computer system;

receiving said first message at said second computer system and generating a key pair comprising an encode key and a decode key for encoding and decoding of said file data;

B1

generating a second message comprising said encode key and transmitting said second message to said first computer system; and

receiving said second message at said first computer system, wherein said encode key in said second message is used to encode said file data.

24. (PREVIOUSLY PRESENTED) The method of claim 23 wherein said secure save command is performed by a component of a graphical user interface presenting command buttons on a user tool bar on said first computer system.

25. (PREVIOUSLY PRESENTED) The method of claim 23 wherein registration functions are performed on said second computer system while said first computer system and said second computer systems maintain a secure link to each other.

26. (PREVIOUSLY PRESENTED) The method of claim 25 wherein authentication functions are performed on said second computer system while said first computer system and said second computer systems maintain a secure link to each other.

27. (PREVIOUSLY PRESENTED) The method of claim 25 wherein said secure link utilizes cryptographic protocols.

28. (CURRENTLY AMENDED) A method of providing secure real time storage and retrieval of data comprising:

maintaining a secure link between a first computer system and a second computer system while performing registration functions on said second computer;

maintaining said secure link between said first computer system and said second computer system while performing authentication functions on said second computer system, wherein said authentication comprises obtaining an identity for said first computer system;

obtaining a secure save command from a user, wherein said secure save command is embedded into a graphical user interface of said first computer system and said user of said secure save command of said graphical user interface initiates a process comprising the steps of:

generating a first message at said first computer system, said first message comprising information corresponding to said file data and said identity, and transmitting said first message to said second computer system;

receiving said first message at said second computer system and generating an encode key for encoding said file data and generating a decode key for decoding said file data;

generating a second message comprising said encode key, and transmitting said second message to said first computer system;

receiving said second message at said first computer system, wherein said encode key in said second message is utilized to encode said file data,

accessing encoded file data by generating a third message at said first computer system, said third message comprising information corresponding to said encoded file data, and transmitting said third message to said second computer system;

receiving said third message at said second computer system, and using said information in said third message to retrieve a record corresponding to said encoded data, said record comprising ~~a~~said decode key for decoding said encoded data;

generating a fourth message comprising said decode key and said information corresponding to said encoded file data, and transmitting said fourth message to said first computer system;

receiving said fourth message at said first computer system, and using said decode key in said fourth message to decode said encoded file data.

29. (PREVIOUSLY PRESENTED) The method of claim 28, wherein said step of generating said first message further comprises:

generating a one way hash function of said file data; and

placing said hash function, information identifying said file data, and user information for a user of said file data at said first computer system in said first message.

30. (CURRENTLY AMENDED) The method of claim 29, further comprising:

obtaining said first message at said second computer;

generating a time stamp, and a digital signature representing said digital time stamp, and said hash function in said first message; and

storing said user information, said information identifying said data, said hash function, said time stamp and said digital signature in a database record.

31. (PREVIOUSLY PRESENTED) The method of claim 30 wherein said second message further comprises:

said time stamp, said information identifying said file data, and said digital signature in said second message.

32. (PREVIOUSLY PRESENTED) The method of claim 28 wherein said encoded file data may be stored at a third computer system.

33. (NEW) A method for providing secure storage of data, comprising:

transmitting a secure save request from a client to a server, said secure save request comprising a file name associated with a data file, an identification value associated with said client, and a one-way hash function of said data file;

generating a storage timestamp at said server;

generating a digital signature at said server based on said storage timestamp and said one-way hash function;

generating, at said server, a first encryption key for encoding and a second encryption key for decoding;

storing said file name, said identification value, said storage timestamp, said digital signature and said second encryption key in a database record;

transmitting a secure save response from said server to said client, said secure save response comprising said file name, said digital signature, and said first encryption key;

using said first encryption key and said data file to obtain encrypted data at said client; and

storing said encrypted data and said digital signature in association with said file name.

34. (NEW) The method of claim 33, further comprising:

transmitting a secure retrieve request from said client to said server, said secure retrieve request comprising said file name, said identification value and said digital signature;

said server comparing said file name, said identification value and said digital signature from said secure retrieval request with said file name, said identification value and said digital signature from said database record;

when said comparing is a match,

generating a retrieval success timestamp and storing said retrieval success timestamp in said database record;

transmitting a secure retrieval response from said server to said client, said secure retrieval response comprising said file name and said second encryption key; and

said client using said second encryption key to decode said encrypted data.

35. (NEW) The method of claim 34, further comprising, when said comparing is not a match:

generating a retrieval attempt timestamp; and

storing said retrieval attempt timestamp in said database record.

36. (NEW) The method of claim 34, further comprising:

said client auditing said database record to obtain an access history comprising said storage timestamp and said retrieval success timestamp.

B1

37. (NEW) The method of claim 33, further comprising:

transmitting a second secure save request from said client to said server, said second secure save request comprising said file name;

said server generating a third encryption key for encoding and a fourth encryption key for decoding, wherein said third encryption key and said fourth encryption key differ from said first encryption key and said second encryption key, respectively.